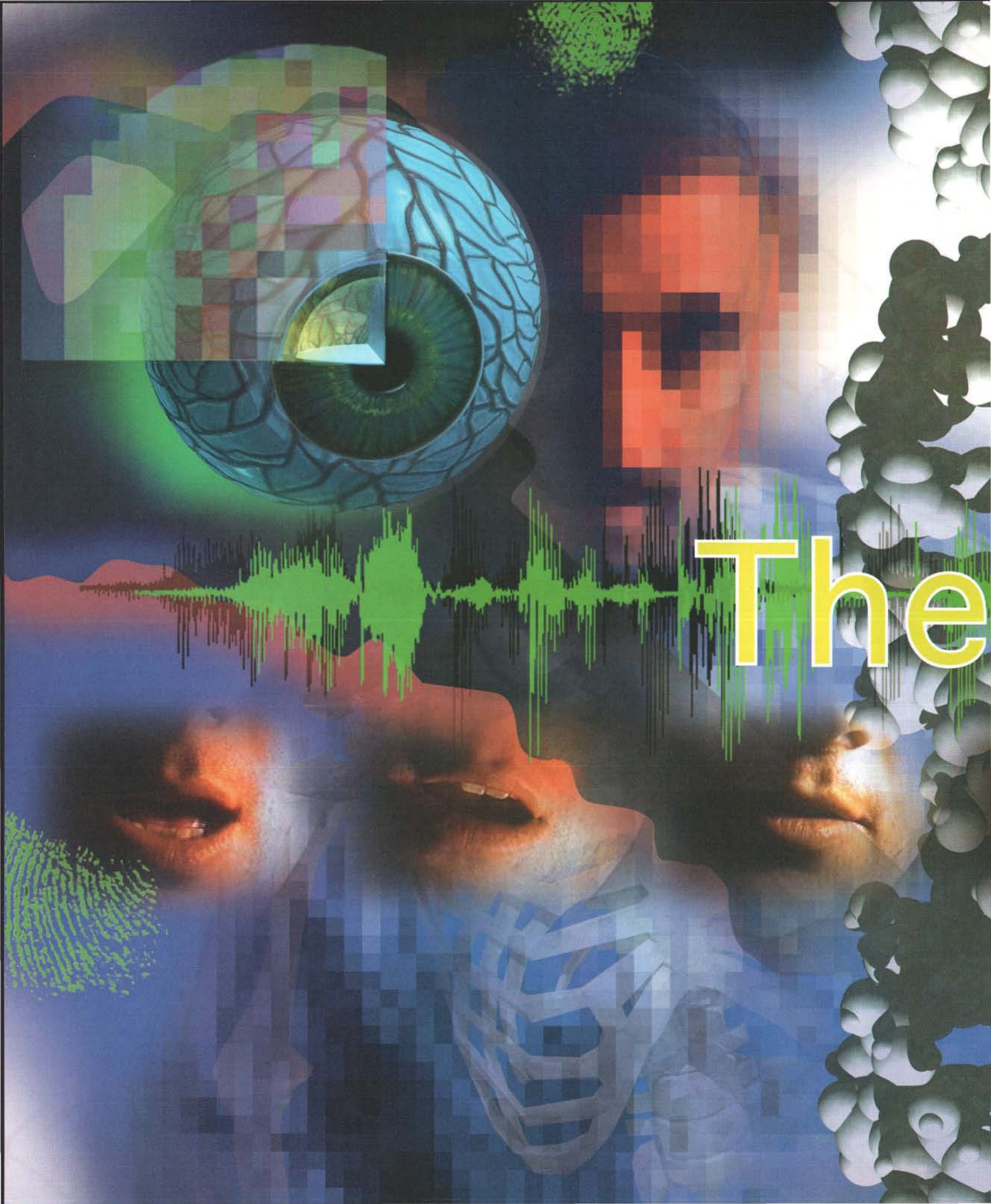
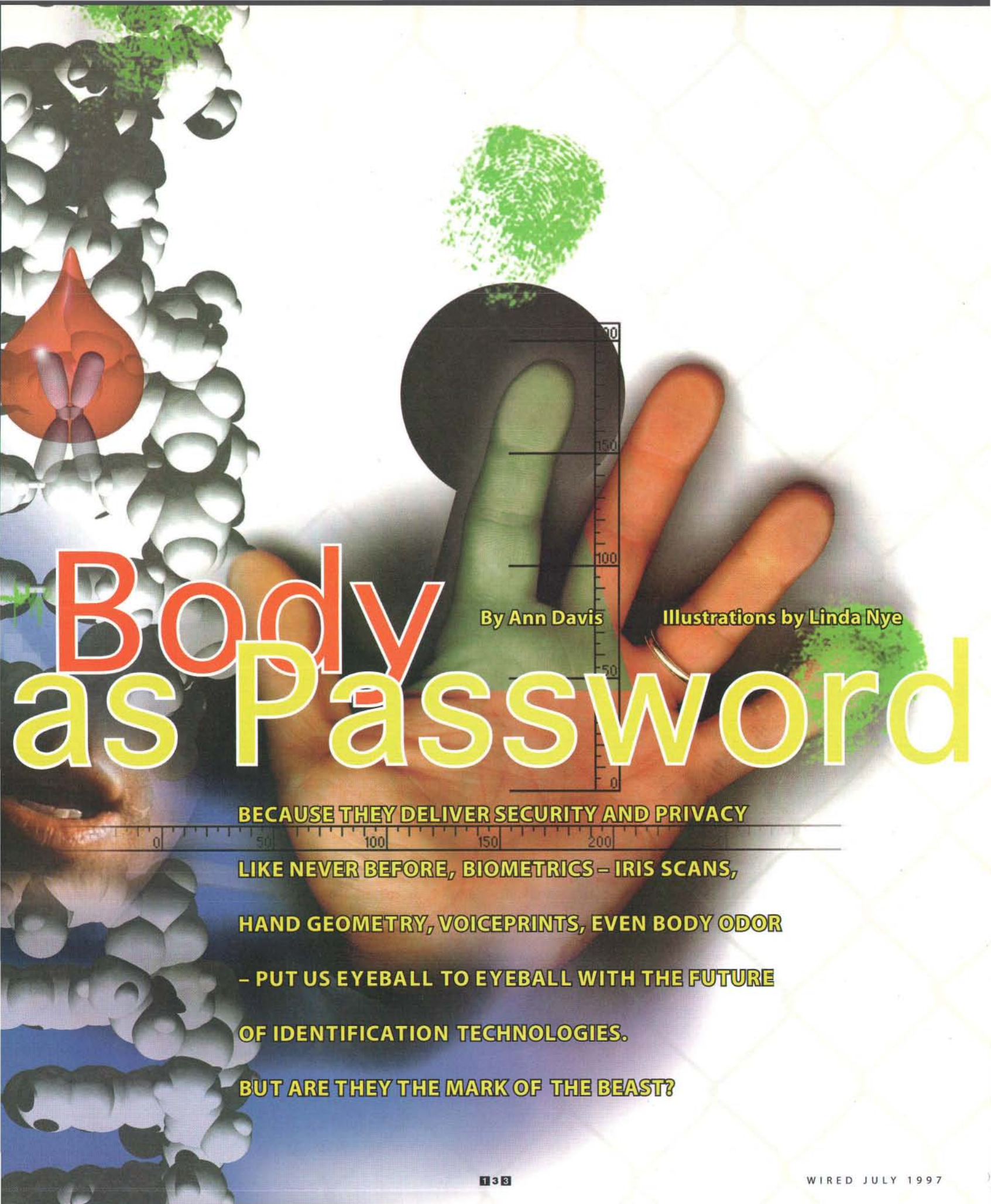




The



Body as Password

By Ann Davis

Illustrations by Linda Nye

BECAUSE THEY DELIVER SECURITY AND PRIVACY

LIKE NEVER BEFORE, BIOMETRICS – IRIS SCANS,

HAND GEOMETRY, VOICEPRINTS, EVEN BODY ODOR

– PUT US EYEBALL TO EYEBALL WITH THE FUTURE

OF IDENTIFICATION TECHNOLOGIES.

BUT ARE THEY THE MARK OF THE BEAST?

Doubters call the digital age dehumanizing, but the joke is on them: the human body lies at the heart of plans to wire banks, streamline government handouts, secure the workplace, even protect your PC. Driver's licenses, credit cards, and office keys as we know them are dinosaurs; the age of the body-part password, or *biometric*, is upon us. Our unique biological characteristics – hand geometry, eye structure, fingerprints, voice patterns, even the way we smell – are

being mapped and digitized as part of a booming new industry.

Biometric technology operates much like the gadgets in spy flicks such as *Mission: Impossible* – computerized scanners confirm a person's identity by examining a biological feature, then matching it with a digital file containing those exact characteristics. Identifiable traits can be physical, such as hand contours or retina patterns. They can be behavioral, such as voice modulation or keystroke typing rhythms. And some can seem a little outlandish: features being tested for singularity among the planet's 6 billion people include knuckle creases, body odors, even acoustic head resonances.

So, are we ready for this form of being digital – to have parts of our fingers, eyes, and speech stored in central databases and traded like commodities by

direct marketers, insurance companies, and government agencies? The smartcard and financial services industries are talking up biometrics as privacy's friend, and experts say biometric IDs are unmatched for security – you can't forge or, presumably, steal someone's body part. Come the millennium, we may be feeding pieces of ourselves into an ever-expanding array of computerized banking files, credit card registries, and state and federal databanks.

Body parts already are used as passwords in various systems, public and private: Inmates must submit to retinal scanning in Cook County, Illinois, coming and going from jail to court appearances. Connecticut and Pennsylvania are two of several states that now use digitized finger imaging to match welfare records with recipients. Frequent travelers crossing into Canada from Montana can zip through an automated voice-verification system run by the US Immigration and Naturalization Service. In the private sector, Lotus employees pass through a hand-geometry scanner to pick up their children from in-house day care. Coca-Cola is using hand geometry at the time clock to prevent workers from "buddy punching" a late colleague's time card.

Just how big is this market? There are now more than 10,000 locations – from bank vaults to blood banks –

where you have to present a body part to walk in the door or access a file. The organizers of the CardTech/SecurTech trade show, an annual event since 1990 now attended by 7,000 participants, say industry revenues are expected to more than triple from almost US\$16 million in 1996 to \$50 million by 1999. The number of biometric devices in use is expected to jump from 8,550 in 1996 to more than 50,000 by the end of decade.

Several products are still in their infancy, and vendors are known to exaggerate the reliability of their machines. But industry leaders claim the free market will eliminate underperformers. In the meantime, lab coats continue to search from head to toe for that elusive unerring yet nonintrusive biometric.

BIOMETRICS: A BLUEPRINT

Enrolling your eye in an IriScan computer is like watching the opening credits of Alfred Hitchcock's *Vertigo*: your giant pupil peers out from the monitor, lashes batting, tear ducts leaking. High-resolution cameras capture the visible surface of the iris from 10 to 12 inches away, then register a 512-byte IrisCode composed of a 15- or 20-line string of numbers and letters that varies each time you look into the lens.

IriScan Inc. of Mount Laurel, New Jersey, markets its technology as "the friendly biometric." Boasting that the iris is "the most unique feature displayed on the human body," IriScan is attracting customers worldwide. Researchers at the National Institutes of Health talked to IriScan about using its machine on lab animals to alleviate the problem of pairing the wrong data with the wrong animal. Tokyo's OKI Electric Industry Company, a leading supplier of automatic teller machines, recently contracted with Sensar Inc. for \$41 million to use IriScan's patented process in developing iris identification for a fleet of Japanese banks.

The next frontier, company gurus say, is computer security. IriScan is developing cameralike eyes that will sit atop a PC or behind the screen, checking at preset intervals whether the person at your keyboard is indeed sporting your iris, with all its distinctive fibers, furrows, coronas, crypts, freckles, rifts, and pits.

Another company wants to do the same with faces. "Your face is your PIN," declares the slogan for the product One-on-One, made by Identification Technologies International in Coral Gables, Florida. The system maps facial contours, recording them as digital codes. A single unit, which runs \$2,000 to \$3,000, includes software and is compatible with a standard PC.

Faces puffy with hangovers or water retention won't trip up One-on-One, claims Identification Technologies spokesperson Kenneth Weiss, but it may be confused by beards, glasses, or similar disguises. Citicorp is testing

Ann Davis (72722.1176@compuserve.com) is a New York-based legal affairs writer.

www.wired.com/5.07/biometrics/

**ARE WE READY FOR
THIS FORM OF BEING
DIGITAL, TO HAVE
PARTS OF OUR BODY
AND SPEECH TRADED
LIKE COMMODITIES
BY BOTH DIRECT
MARKETERS AND
THE FEDS?**



the system for use at its bank machines.

Moving down the body, hands and fingers hold even more promise. The market for digital finger imaging is well-developed because of a strong demand from law enforcement. Identicator, a leader in the field of digital finger imaging based in San Bruno, California, sells its fingerprint scanners for \$400 to \$1,000. But Identicator president Oscar Pieper hopes to mass-market his machines for \$30 to \$50 within a few years. Already, MasterCard is running television commercials featuring Identicator scanners. "Since the last thing you need is one more number to remember, MasterCard is developing the single-digit PIN code," the ad proclaims. "Some-day a computer chip in your card will recognize your unique mark."

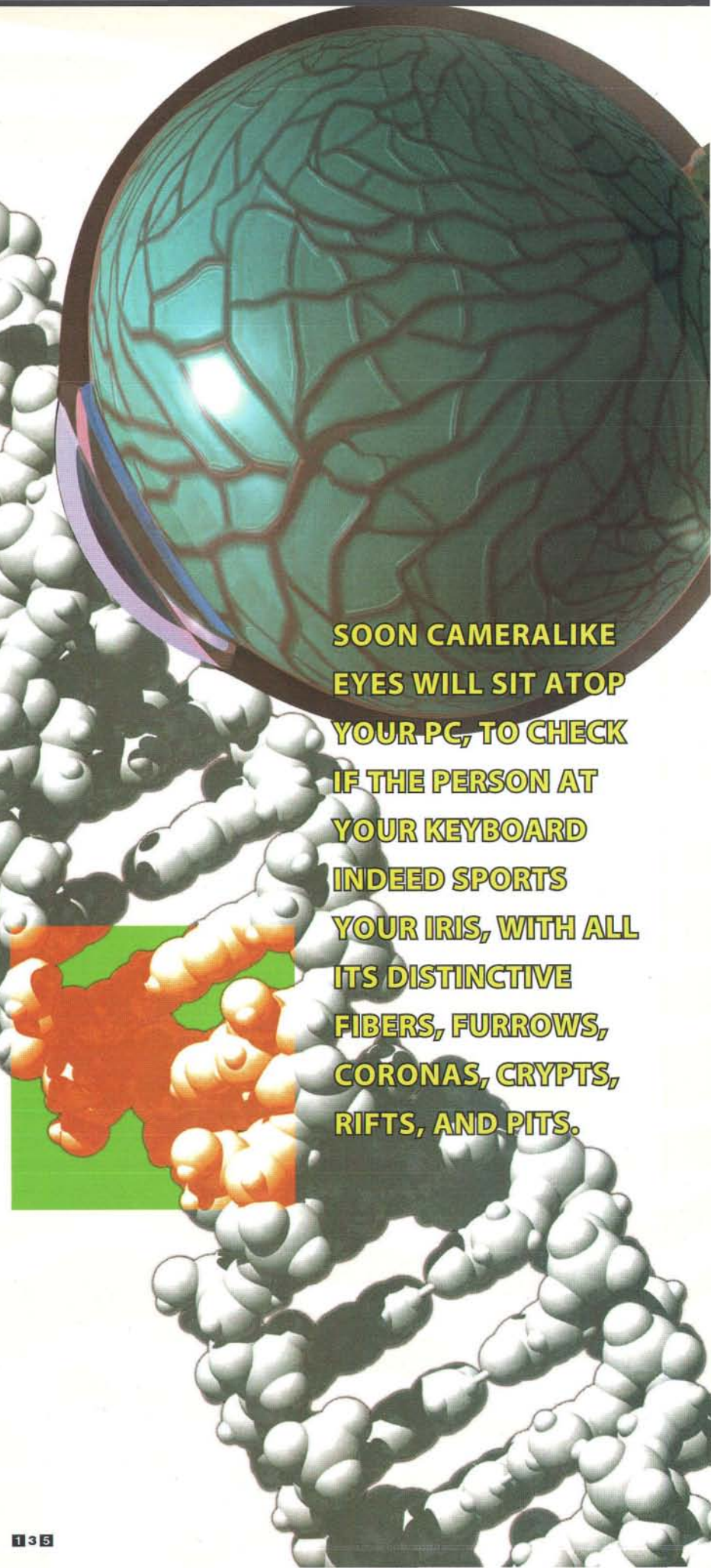
Another technology exploiting the uniqueness of our digits is finger geometry. Scanning the dimensions of one or more digits, these machines typically cost about \$1,500. In 1995, The Walt Disney Company contracted with the Swiss firm BioMet Partners to test a 3-D, two-finger geometry device – the Digi-2 – at entrance turnstiles for holders of season passes to Walt Disney World in Orlando, Florida.

The first modern biometric device, which debuted more than 20 years ago at the Shearson Hamill investment bank on Wall Street, was a hand-geometry reader that measured finger length. Since then, a best-seller has emerged: the ID-3D Handkey from Recognition Systems Inc. The device scans fingers plus the tops and sides of the hand with a video camera, then converts the data with compression algorithms. Nearly 4,000 of the machines were sold in 1996. They're used at immigration checkpoints at San Francisco International Airport, for access to the Colombian legislature, and to verify the identity of donors at sperm banks.

Some vendors think the answer is not at your fingertips, but on the tip of your tongue. Voice verification is already one of the most reliable biometrics, say government researchers at the National Security Agency, which monitors its use in numerous federal computer facilities. Several states use voice recognition for parolees on home detention.

Mirroring its system in place on the Canadian border, the Immigration and Naturalization Service has conceived of a commuter lane with a "voice box" into which frequent travelers across the Mexican border will speak a phrase of their choice. (When it dawned on the Feds that a drive-through voice checkpoint might miss illegal aliens hiding in vehicle freight compartments, the INS asked a federal research lab to develop sensors that can detect heartbeats hidden in a cargo hold.)

According to *Personal Identification News*, a respected industry newsletter, major corporations, including Martin Marietta, GM, and Hertz, are protecting their computer facilities with voice technology. Voice systems also guard private estates from Silicon Valley to Latin America. 174 ►



**SOON CAMERALIKE
EYES WILL SIT ATOP
YOUR PC, TO CHECK
IF THE PERSON AT
YOUR KEYBOARD
INDEED SPORTS
YOUR IRIS, WITH ALL
ITS DISTINCTIVE
FIBERS, FURROWS,
CORONAS, CRYPTS,
RIFTS, AND PITS.**